

REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 18-37 are in this case

Claims 18-37 were rejected under 35 U.S.C. §102(e) as being anticipated by Candelore et al. US patent 6,061,449 (hereinafter Candelore)

While continuing to traverse the Examiner's rejections, and without in any way prejudicing the patentability of the rejected claims, the Applicant has, in order to expedite the prosecution, chosen to amend the claims thereby rendering moot Examiner's rejections.

SUMMARY OF EXAMINER INTERVIEW

An telephone interview with Examiner Williams was held at 11:10 EST on February 13, 2007 . The topic of discussion was a proposed amendment to Claim 18 and whether the proposed amendment is sufficient to overcome the rejection under 35 U.S.C. §102(e) as being anticipated by Candelore. Applicant explained that the designating is performed by a user, such as an owner of software or digital content to mark or flag locations at which the arming step is performed. Examiner indicated that the language in claim 18 of designating ...critical locations indicates or hints at further steps of the claimed process but is not sufficiently substantive in and of itself to be considered a novel step over Candelore. Examiner suggested that Candelore does teach designating ...critical locations, in column 28. Applicant explained that Candelore deals with the problem of securing RAM memory and the blocks of Candelore are blocks of memory defined by absolute RAM addresses, not locations (or relative addresses) within an executable program or data. Applicant further explained that the paragraph beginning on line 28 of column 28 of Candelore discusses efficiencies regarding how a program should be stored within RAM memory after the cipher block chaining scheme of Candelore is set up, so that single instructions do not cross blocks of memory. By the end of the interview, Examiner and Applicant agreed that claim language such as marking locations or flagging locations in a program file or data is more substantive than designating, that Candelore does not teach marking or flagging locations in a program file and Examiner is willing to reconsider the rejection including such a step.

Amendments to the Claims

Applicant has rewritten the claims to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention more patentably over the prior art. Specifically, the step *designating* has been replaced by *marking*; the *modified executable program file* has been replaced with *secured file*. The *executing* step of claim 18, has been rewritten into a "wherein" clause because the execution is actually a result of the claimed process. Claim 33 has been canceled because the limitation is already included in the *marking* step of claim 18. Claim 37 has been rewritten in dependent form.

New Claim 38

A new claim 38 claims the invention in terms of data, as defined in the specification to include software and/or digital content. Otherwise limitations of claim 38 are similar to those of claim 18.

Rejections under 35 U.S.C §102

The References and Differences of the Present Invention Thereover:

Prior to discussing the claims, Applicant will first discuss the references of the prior art of record and the novelty of the present invention and its unobviousness over the references.

By way of introduction, Applicant respectfully affirms that there are fundamental differences between Candelore and the present invention. The disclosure according to Candelore is based on dedicated hardware ("secure circuit", column 1 lines 32-47), Figure 1 Candelore). The method of Candelore protects memory, *e.g.* RAM in a computer using a technique known as "cipher block chaining". In cipher-block chaining, the RAM memory is divided into blocks. The blocks are necessarily of equal size, for instance of 8 bytes (see Candelore column 6 line 50). RAM memory for instance 80,000 bytes is divided into 10,000 blocks, each block of 8 bytes. Each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to

that point. To make the cipher unique, an initialization vector typically dependent on the processor is used in the first block.

Applicant has reviewed Candelore again, and has amended the claims herein to more particularly define the invention more distinctly from Candelore's disclosure. Specifically, Candelore does not teach *marking a plurality of locations within the executable program file (or data) by placing a plurality of flags at said locations*. The disclosure of Candelore does not consider *locations within the executable program file or data stored*. The division into blocks, according to Candelore is performed in RAM memory based on absolute memory addresses while there are no data or program files stored in the RAM memory. Hence Candelore, does not perform a step of *marking a plurality of locations within the executable program file (data) by placing a plurality of flags at said locations*. Similarly, Candelore has no step analogous to: *arming the executable program file (data), thereby producing the secured program file by including a plurality of software procedures at said locations*. The block-by-block encryption of Candelore is built into hardware before there is any data or program file stored in the RAM memory. Hence Candelore does not have a step of *arming ... by includingsoftware procedures at said locations* since the locations and the program (data) are non-existent in Candelore.

Applicant respectfully submits that independent claims 18 and 38 are patentable over Candelore based on the following rulings.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)

To serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence. Such evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co. USA v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749 (Fed. Cir. 1991)

Extrinsic evidence may be used to explain but not expand the meaning of terms and phrases used in the reference relied upon as anticipatory of the claimed subject matter. *In re Baxter Travenol Labs.*, 952 F.2d 388, 21 USPQ2d 1281 (Fed. Cir. 1991)

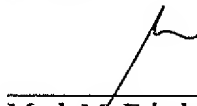
Novel physical features of Independent claims 18 and 37**Produce New and Unexpected Results**

Applicant wishes to point out "new and unexpected results" of using distinct steps *marking* and *arming*. *Marking* is used mark the software parts to be protected and generate a flagged software file. The flagged software doesn't include any additional functionality comparing to the original un-flagged software. At a later stage, during the *arming* step, a machine code containing security functionality is inserted into the marked locations at the flagged software. The use of two distinct steps *designating and arming* is essential for commercial utilization, because the provider of the copy protection (*e.g.* a CD replication facility) doesn't wish to grant to the software vendor, author or copyright owner fully functional tools that can be used for an unlimited number of copies. Instead, the tools delivered to the software vendor do not add any functionality, but just mark the locations in the software to be protected. The copy protection provider can then perform the arming process on the number of copies requested by the software vendor (*e.g.* replicating 1000 CDs containing the armed software) and charge the software vendor for the copy protection service according to the number of copies on which the arming process was performed. This process is illustrated in figures 1d and 1e.

The present invention is a method for authenticating and protecting digital data from illegal copy and use, which is independent of the processor or any other hardware. Thus, protected software according to the present invention can be executed on any computer hardware.

In view of the above amendments and remarks it is respectfully submitted that independent claims 18 and 39 and claims dependent therefrom are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,



Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: Feb 14, 2007